

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Software-efficient Stream Ciphers Using Linear Masking

the specification of which (check one)

☒ is attached hereto.

☐ was filed on \_\_\_\_\_ as United States Application Number \_\_\_\_\_

or PCT International Application Number \_\_\_\_\_

and was amended on \_\_\_\_\_ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)	Priority Claimed
(Number) _____ (Country) _____ (Day/Month/Year Filed) _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
(Number) _____ (Country) _____ (Day/Month/Year Filed) _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
(Number) _____ (Country) _____ (Day/Month/Year Filed) _____	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

(Application Number) _____	(Filing Date) _____
(Application Number) _____	(Filing Date) _____

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) _____	(Filing Date) _____	(Status) (patented, pending, abandoned) _____
(Application Serial No.) _____	(Filing Date) _____	(Status) (patented, pending, abandoned) _____

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

MannyW. Schecter (Reg. 31, 722), ChristopherA. Hughes (Reg. 26, 914), JohnE. Hoel (Reg. 26, 279), JosephC. Redmond, Jr. (Reg. 18, 753), DouglasW. Cameron (Reg. 31, 596), LouisP. Herzberg (Reg. 41, 500), StephenC. Kaufman (Reg. 29, 551), DanielP. Morris (Reg. 32, 053), PaulJ. Otterstedt (Reg. 37, 411), LouisJ. Percello (Reg. 33, 206), MarianUnderweiser (Reg. 46, 134), RichardM. Ludwin (Reg. 33, 010), MarcA. Ehrlich (Reg. 39, 966), RobertM. Trepp (Reg. 25, 933), Kevin M. Jodan (Reg. 40, 277), DerekJennings (Reg. 41, 473), Gail Zarick (Reg. 43, 303),

Send Correspondence to: Louis J. Percello, Intellectual Property Law Dept., IBM Corporation,  
P.O. Box 218, Yorktown Heights, New York 10598

Direct Telephone Calls to: (name and telephone number) Louis J. Percello (914)945-3145

Don Coppersmith

Full name of sole or first inventor

X Don Coppersmith  
Inventor's Signature

2/4/2002  
Date

56 Ferris Place, Ossining, NY 1062 USA

Residence

USA

Citizenship

Same as above

Post Office Address

MAR 26 2002

Docket No YOR920020025

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

**COPY OF PAPERS  
ORIGINALLY FILED**

Shai Halevi

Full name of second joint-inventor, if any

X Shai Halevi  
Inventor's signature

X 2-7-2002

Date

1602 Old Country Rd., Elmsford, NY 10523  
Residence

Israel  
Citizenship

Same as above  
Post Office Address

Charanjit Jutla

Full name of third joint-inventor, if any

X Charanjit Jutla  
Inventor's signature

X 2-7-2002

Date

298 Nob Hill Rd., Elmsford, NY 10523  
Residence

India  
Citizenship

Same as above  
Post Office Address

## Assignment

Whereas, I/we

INVENTOR  
AND COUNTY

(1) Don Coppersmith  
County: Westchester

of: Ossining  
State: New York

(2) Shai Halevi  
County: Westchester

of: Elmsford  
State: New York

(3) Charanjit Jutla  
County: Bronx

of: Elmsford  
State: New York

has invented certain improvements in

TITLE Software-efficient Stream Ciphers Using Linear Masking

executed, respectively, a United States patent application therefor on

DATE THAT

INVENTOR  
INVENTOR  
INVENTOR  
INVENTOR

(1) Feb. 4, 2002,  
(2) 2/7 2002,  
(3) Feb. 7 2002.

SIGNED THE  
DECLARATION

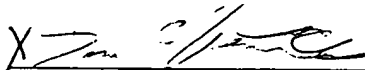
Whereas, INTERNATIONAL BUSINESS MACHINES CORPORATION, a corporation of New York, having a place of business at Armonk, New York 10504, (hereinafter called IBM), desires to acquire the entire right, title and interest in the said application and invention, and to any United States and foreign patents to be obtained therefor;

Now therefore, for a valuable consideration, receipt whereof is hereby acknowledged, we, the above named, hereby sell, assign, and transfer to IBM, its successors and assigns, the entire right, title and interest in the said application and invention therein disclosed for the United States and foreign countries, and all rights of priority resulting from the filing of said United States application, and we request the Commissioner of Patents to issue any Letters Patent granted upon the inventions set forth in said applications to IBM, its successors and assigns; and we hereby agree that IBM may apply for foreign Letters Patent on said invention and we will execute all papers necessary in connection with the United States and foreign applications when called upon to do so by IBM.

Signed and sealed

CITY AND  
DATE

(1) at Yorktown, NY.  
on Feb. 4, 2002

X 

( Don Coppersmith )

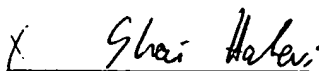
FIRST NAME MIDDLE INITIAL LAST NAME

SIGNATURE

Signed and sealed

CITY AND  
DATE

(2) at Hawthorn, NY  
on Feb. 7, 2002

X 

( Shai Halevi )

FIRST NAME MIDDLE INITIAL LAST NAME

SIGNATURE

**Signed and sealed.**

CITY AND  
DATE

(3) at Hawthorne  
on Feb 07, 2002

X                      SIGNATURE  
 ( Charanjit                                  Jutla )  
 FIRST NAME       MIDDLE INITIAL     LAST NAME